Provided for Public Comment: Thursday, September 26, 1996

Governor's Work Group on Commercial Access to Government Electronic Records

DRAFT POSITION PAPER ON QUESTION 1

The first of three position papers prepared for the consideration of the Work Group

TOWARD A POLICY FRAMEWORK FOR THE COMMERCIAL RELEASE OF ELECTRONIC PUBLIC RECORDS

I. Introduction.

> *How, and under what circumstances, should public records in electronic format be released for business or commercial purposes?*

Under Washington State law, public records that are lists of individuals cannot be released for commercial purposes, unless there is a specific statutory authorization to do so (RCW 42.17.260(9)). The 1996 legislature introduced and passed two bills, HB 2790 and HB 2604, that would have further expanded the growing number of exemptions to this prohibition.

Together, the bills raised what Governor Mike Lowry viewed as "serious questions that state policy now fails to answer." On March 30, 1996, the Governor vetoed the bills and announced that he would convene a Work Group to review current state practices and policies related to the commercial release of public records.

The Governor expressed concern over the cumulative effect of hundreds of exemptions over twenty-four years -- compounded by the impact of new digital technologies -- on how government handles public records. "As state government responds to emerging technologies, it is likely that we will have to modify the way we control and disburse the information we hold[1]."

His instructions to the Work Group were clear: "The charter of the Work Group is to recommend whether and under what circumstances government records in electronic format should be released for commercial, profit-making purposes, with particular emphasis on safeguarding the privacy rights of individuals who are subject to those records."

At its first public meeting, the Governor told the Work Group that commercial access to public records represents a growing question in the electronic age. Indeed, public policy tends to lag behind societal developments. The lag is even more pronounced

[1] HB 2604 (Full Veto)

in dealing with electronic records because of relentless technological change. The rapid advances related to the Internet and other digital technologies often eclipse the public sector's ability to stay abreast of the technological developments and account for their social impact.

The Governor asked the Work Group to send the clearest possible message by developing a coherent statewide policy that balances legitimate business and government interests with personal privacy concerns.

This paper reflects the direction of the Work Group as it creates the framework for a single, coherent, statewide policy on commercial release of public records. The group recognizes that the criteria for determining permissible commercial use of public records must be kept relatively simple. In the group's view, permissible use is measured against what is disclosable under the law and hinges on the question of public benefit.

II. The Public Benefit of Commercial Access to Government Electronic Records.

The Legislature has found "that government information is a strategic resource and needs to be managed as such and that broad public access to non-restricted public information and records must be guaranteed.[2]"

Broad, legitimate and authorized public access clearly constitutes a public benefit. The Open Records Act was passed by citizen initiative in 1972 to codify those benefits -- providing citizens with the information they need to hold government to account.[3] The Open Records Act balances the mandate for open government with a provision to exclude those records whose release would be "highly offensive to a reasonable person and of no legitimate public concern.[4]"

Commercial release involves a broad spectrum of public records -- from legislative and regulatory information to personally identifiable information. The latter is allowed only through legislative exemption. There are more than 200 such exemptions in place in Washington state. The end result is a system that can treat the same information differently from agency to agency. Information that is prohibited from release under one government program is available from another. The inconsistency extends to the treatment of records between programs within agencies. For example, certain medical records are restricted under state law but may be open to disclosure under audit provisions of the federal Medicare program.

The patchwork quilt of release provisions -- overlapping in some areas and threadbare in others -- causes uncertainty and confusion for the agencies that are entrusted with the proper management of public records. If the trustees of public records are

[2] RCW 42.17.261 (1994)
[3] As will be discussed in a subsequent position paper on Question 3, commercial release may play a vital role in sustaining electronic public access systems.
[4] RCW 42.17.300

confused, it is understandable that individuals (the subjects of those records) are expressing growing concern about how information about them is handled. The uneven statutory provisions governing release of public records is complicated by issues related to technological change and commercial release.

1. Commercial Release

Commercial release itself cannot be treated as a monolith because the nature of commercial interests varies widely. Some private interests use public records to comply with regulatory or legal requirements. Others are full service information resellers -- such as Lexis-Nexis, TRW and Commercial Information Systems (CIS) of Portland.[5] These information resellers typically apply custom indexing and searching capabilities to a broad range of data, from both public and private sources.

In written and oral submissions to the Work Group, CIS and its clients advocated the identification of "permissible uses" and permitted users of public records in electronic form. Given the Work Group's charter, any discussion of permissible uses and users necessarily begins with the notion of public benefit. Again, the universe of records under discussion is defined by what is disclosable under the law, coupled with the subsequent exemptions.

As stewards of public records, one of government's responsibilities is to derive benefit for citizens through the proper use of data. Public benefit is derived through direct governmental use of public records, as is the case when data is used by planners to deliver services more effectively or to anticipate future demands for infrastructure. Public benefit can also be derived through certain private sector uses of public records. For example, there is a strong public safety interest in notifying vehicle owners of a recall in a timely fashion. The recall is done on behalf of a manufacturer by an information reseller using public records.

Government is often the holder of the unique and authoritative record to which all other records refer. To expand on the example given above, the Department of Licensing (DOL) holds the authoritative records on registered motor vehicles in the state. The use of DOL data by a commercial information reseller to notify vehicle owners of a recall or safety defect has a demonstrable public benefit. The auto manufacturer, the information reseller working on its behalf, insurance companies, the government and the public all derive benefit from the initial release of those motor vehicle records.

There are also clear (albeit different) public benefits derived from the commercial release of land title records for sellers, buyers, realtors and lenders. The records provide the legal underpinnings of significant economic transactions. All parties have an interest in verifying the status of property before and after its sale. Again, government holds the unique and authoritative records.

[5] CIS actively supported the passage of HB 2790, one of the bills vetoed by the Governor in March 1996.

Public records are of considerable value in planning both public infrastructure and private enterprise. Demographic, labor market and import/export data are important in projecting the demand for daycare facilities, schools, retirement centers and transportation infrastructure. The data is also instrumental in siting decisions for manufacturing plants, housing developments and retail outlets.

2. Distinction Between Commercial and Business Use

Another category of use demonstrates the subtle but important distinction between commercial and business use.

The Open Records Act prohibits the release of lists of individuals for commercial purposes. In opinions by the Attorney General, commercial purposes are defined as "profit expecting activity." Under such a definition, a list of vintage car owners could be released to an antique car club but not to an auto dealer because the dealer has a profit expectation and the club does not.

Beyond the distinction between commercial interests and the not-for-profit sectors, there is a distinction to be made between commercial and business use of public records.

Many businesses rely on a second or third party to corroborate information given to them. Importantly, such verification is often needed to comply with government regulations. Hiring decisions provide a number of illustrative examples in this regard. Transportation companies must check on applicants' past driving history. Schools and daycares must ensure that applicants do not have any criminal history that would put children in harm's way.; Employers are required to check an applicant's eligibility to work in the United States.

In all these cases, public records are used to verify certain information in order to conduct business in a legal and responsible manner. It follows then that government has a duty to release the information needed to comply with obligations it imposes on the private sector.

In contrast, public records are sometimes used for unsolicited business contact or other purposes where there is no demonstrable public good. Such commercial use, often done without the subject's knowledge or consent, includes securing lists for the purpose of direct mailing, or the creation of personal dossiers or profiles through the compilation of data from once discrete databases.

In any commercial release of public records, there is likely to be a mixture of public and private benefit. In some instances, there is a predominant public benefit. In other cases, the public benefit is incidental to a predominant private benefit. In still other cases, the public and private benefits are balanced.

The place of any particular commercial or business use on the continuum between public and private benefit has important policy and planning implications. To the degree that commercial release lends itself to public benefit, those uses should be supported by the release of the needed information. As the pendulum swings the other way, in instances where any public benefit is only incidental to a predominantly private interest, the release of records should be restricted.

The planning issues follow from the broader policy concerns. As agencies face increased demands for services from the public while budget levels remain static (or shrink), the support of electronic access systems must be justified in terms of public benefit.

3. Efficiency

A number of agencies, together with Association of Washington Cities and the County Officials Association, told the Work Group that records requests are growing rapidly as electronic records become the norm. Agencies report that servicing requests often divert resources away from the agency's legislatively-mandated mission. The departments of Licensing and Health have expressed particular concern that any test for commercial release factor in the cost implications of producing the records in such a way that comports to state law and is usable to an external party. Such concerns are not always reflected in discussions of greater government efficiencies through the use of technology.

Proponants of HB 2790 said its provisions would give goverment more powerful and user friendly capabilities in manipulating electronic public records. Under the bill, a private sector interest would add value to those records and provide government with access to the improved data.

As envisioned, private sector participation would allow government greater access to state-of-the-art technology and the ability to better manage its data. Private sector participation would also help mitigate the technology-related risks and costs. To be clear, such partnerships are not necessarily inconsistent with the proper stewardship of sensitive information with which government has been trusted.

The use of private-sector consultants and contractors to improve data or enhance systems to better manage data is an everyday (and long established) practice by state agencies. Given that data and system improvements can be done legally without any additional legislative authorization, the Work Group may want to consider how HB 2790 would have been implemented.

It is unclear how HB 2790 impacts the ownership of, and control over, public records. So long as the records remain a public trust (as they now do under agreements with private vendors), government has the authority to prescribe permissible and non-permissible uses. If the rights to those records were to be transferred as part of any value-

added arrangement, the government (as the public's trustee) would lose any right to control use by second or third parties. Its ability to curb abuse would likewise be lost.

By itself, efficiency may be an inadequate test for justifying the commercial release of public records. However, efficiency should be included in a broader test of public benefit.

One of the challenges faced by the Work Group is how to deal with secondary use -- and in some cases, abuse -- of public records even when their initial release is justified by the public benefit test.

III. Stewardship of Public Records.

As discussed above, the categories of acceptable use include:

- information to hold government accountable;
- information to comply with government regulations;
- information to support private-sector decision-making; and
- information needed to deliver services on behalf of government.

Government agencies are responsible to three "publics": (1) the taxpayers of Washington state, (2) the millions of people served by agencies, and (3) the entities with which some state agencies contract to provide services to citizens on their behalf. Each "public" has a different need for information -- and often a different expectation about how the information will be handled. The degree to which those expectations differ often only becomes clear after the fact.

An example from health care may help illustrate what is, in practice, a "stair stepped" approach to handling certain sets of sensitive data. A health care provider needs a certain detail of information to treat a patient. An insurance company will need some information about the treatment in order to pay the claim. An employer may need to verify that a treatment has taken place to ensure that the patient is eligible for sick leave. The citizen -- who is simultaneously the patient, claimant, employee and tax payer in this scenario -- has a legitimate expectation that her records will be kept confidential except to satisfy the specific needs of the other parties.

1. Original Orbit

Public benefit eludes easy definition. A useful model for delineating among potential uses based on their public benefit was introduced by a Work Group member. Under this model, the highest public benefit is realized when the records are used within the orbit for which they were collected[6]. For example, the highest public benefit from health records is when they are used within their original orbit -- that is, the delivery and planning of health services. The vehicle recall example used above would also fit within the original orbit of motor vehicles records because it represents an extension of the public safety role performed by the Department of Licensing.

However, the subsequent use of those motor vehicles records for direct mail campaigns or siting decisions for retail outlets would be outside the original orbit. The use of public records extend beyond the original orbit raises questions of secondary use which, as trustees of the records, government must address.

2. Secondary Use

There is no consistant policy governing secondary use of public records under statute. Practices by state agencies and local governments vary widely. Once released, the subsequent use and disposal of public records with personally-identifiable information (and the prospect of secondary use) is a matter of growing public concern[7]. Depending on the jurisdiction, and the precise nature of the information, its disposal after initial release may be a matter covered by statute, regulation, contract or left to the vagaries of the marketplace.

The importance of, and public concern over, secondary use of electronic public records has been underscored repeatedly during the Work Group's brief tenure. First came the computer enthusiast who posted the entire Oregon DMV database on the World Wide Web[8]. Second, federal law enforcement raised the ire of non-consenting third parties whose credit histories were used as bait in a sting operation[9]. The third case in as many months came in September when the information reseller Lexis-Nexis launched P-Trax. The service allows users to search for the current and former addresses, phone number and, in some cases, the maiden name of most anyone. After a storm of protest, the ability to retrieve Social Security numbers through P-Trax was removed eleven days

---

[6] The original orbit model appears to be consistent with the emerging *Fair Information Practices* which will be addressed by Dr. Cavoukian during the September 26, 1996, videoconference.

[7] Matters related to the safeguarding of personal information will be discussed in a subsequent position paper on Question 2.

[8] William McCall, "Vehicle files on Internet draws anger," *Tacoma News Tribune*, Aug. 8, 1996. The Oregon case is not, strictly speaking, an example of commercial use because the provider is not charging for access. There are other such services -- such as Internet DMV -- that provides on line searching of a number of state databases for $20 to $35 per search.

[9] Jim Newton, "Credit-card holders cry foul that accounts used in sting," *Seattle Times*, Aug. 30, 1996.

after the service's launch. In its defense, the company said it was only using data obtained from public records.[10]

These three cases are among the most recent revelations about the exposure of personally identifiable information that individuals have assumed was being safeguarded. These individuals, and certain interest groups speaking on behalf of the public at large, are asking serious questions about how much personal information is considered "public." The rules (and the law) have not changed -- the technology has. Indeed, digitization has forced these issues onto the table. The digital environment destroys the inherent protection afforded to people in an earlier analog era -- gone are the cumbersome paper-based systems that made it difficult to get at and manipulate personal information.

3. Misuse and Abuse

A member of the Work Group portrayed the misuse of digitized personal data in graphic terms -- referring to it as "high tech assault." In the Group's view, there is no interest in creating a new bureaucracy to handle data. In its view, it is more efficient to deal with abuse using sanctions after the fact. Ironically, the only sanctions in the Open Records Act are against failing to release. There are no enforcement provisions under the Act to mitigate against abuse related to improper release of lists of individuals.

A white paper on enforcement issues related to the Open Records Act has been prepared by Chip Holcomb, Senior Assistant Attorney General, and was included with the September 26 meeting materials.

The problem here extends beyond the Act's silence on providing disincentives to the abuse of public records. A change in the underlying technology that holds and manages records is challenging the assumptions that have been embedded in our print-based culture since Gutenberg.

IV. Digital Records: Decomposition of the Document.

The Open Records Act does not make a distinction between paper-based records and those in electronic form. Why would it? A quarter century after its passage, the impact of digitization is only now being understood by industry, government and individuals. The founder of the MIT Media Lab, Nicholas Negroponte, contends that digitization is not just a technological change -- it is a societal transformation. To apply Negroponte's language to the present case, public records are being transformed from "atoms" (paper) to "bits" (electronic).

Digital technology fundamentally changes the nature of records. The change is rooted in the fact that "bits commingle effortlessly."[11] That fact brings with it considerable promise -- and the risk of dangerous pitfalls -- to the proper stewardship of public records.

---

[10] Thomas E. Weber, "Lexis-Nexis Database Sparks Outcry on the Internet about Privacy Issues," *Wall Street Journal*, Sept. 19, 1996.

In the shift from paper-based to electronic records, there has been the loss of the contextual (*See Figure 1*). People may still fill out forms in conducting transactions with government. However, that paper record begins to decompose the instant discrete pieces of information from that single document become data elements in a data base. In fact, the paper form as a container of data has largely been replaced as the "unique copy" of the record by a series of digital fields. Because "bits commingle effortlessly," any combination of data elements can be manipulated in ways that: 1) improve efficiencies in service design and delivery, but 2) may not fully be understood by the subjects of the original record.

While information provided on a paper form will remain static over time, the digital environment is dynamic. In electronic form, data elements can be updated, changed or corrupted over time. The malleability of electronic data raises questions related to the temporal elements of public records -- namely, version and transaction control. These issues tend to escape widespread attention, with the possible exception of the Information Technology (IT) community, but raise significant stewardship concerns at the public policy level.

Figure 1: Document Decomposition

[11] Nicholas Negroponte,*Being Digital*, New York, Albert A. Knoff, 1995:18.

V. Software Development and Public-Private Partnerships.

This position paper has already made a number of important distinctions -- public vs. commercial access; commercial vs. not-for-profit use; commercial vs. business use; public vs. private benefit; and, analog vs. digital records. Within the realm of digital records, it is necessary to make at least one additional distinction -- between the electronic records and the software that creates them.

Digital records do not exist in a vacuum. They are created, maintained, safeguarded, manipulated and updated by computer software. The software represents a significant public investment. The software is made up of millions of lines of code that create virtual containers for the data (*see Figure 1*) -- and whose design sets out the relationships of data within and among those containers. The codification of those relationships in software is an increasingly complex and risky business.

To gain access to state-of-the-art software development expertise, state agencies have an established practice of contracting with private sector firms. There are no prohibitions against public entities using private contractors to add value directly or indirectly (the latter through building or enhancing government IT systems to better manage data).

Done properly, such arrangements can produce more advanced systems at less cost to taxpayers. To further contain costs, the relationship between public agencies and vendors can be cast in terms of a public-private partnership. Under such partnerships, risks and rewards are shared with the private contractor. While the records themselves remain a public trust, the software developed to manage them is jointly owned by the state and the private partner.

Under joint ownership, the state has guaranteed access to the software needed to manage its data. For its part, the private partner is able to leverage the research and development costs it absorbed on a given state project by applying all or part of the code on other projects with other customers.

A survey by the National Association of State Legislators reports that twenty states have exempted software from their open records legislation. Some parties are concerned that a software exemption may limit the public's access to its records. In the Work Group's view, this concern can be addressed through contractual provisions that ensure that the state (as trustee) will have full and perpetual access to the jointly-owned software for governmental use -- including public access.

A software exemption would allow the state to protect the public investment in proprietary software, leverage its resources through public-private partnerships and other such strategic alliances, and ensure that the software that supports public records can be maintained, enhanced and refurbished as necessary.

VI. Conclusion.

In answering the question, *How, and under what circumstances, should public records in electronic format be released for business or commercial purposes?*, the Work Group finds:

- the universe of public records subject to disclosure is defined by statute.

- public records are a public trust. The control or ownership of those records should not be transferred to other parties.

- the highest public benefit from public records is when they are used for the purposes for which they were collected. The public benefit test of remaining within "original orbit" is true for governmental, commercial and business uses of information.

- permissible commercial or business use should meet a test of demonstrable public benefit.

- the Open Records Act is silent on sanctions against improper initial release of public records -- and on misuse related to secondary use.

- digital technology changes the nature of public records themselves, bringing with it the prospect for greater governmental efficiencies and the need for additional safeguards to protect personally identifiable information.

- the Open Records Act does not distinguish between public records and the software that creates and maintains them in a digital environment. In the absence of any protections for the significant public investment in proprietary software, the state faces difficulties in ensuring the future availability, enhancement and refurbishment of these systems.